Postulates of quantum mechanics

Postulate 1. Associated to any isolated physical system is a unitary space known as the *state space* of the system. The system is completely described by its state vector, which is a unit vector in the system's state space.

Two vectors which differ just by a factor $e^{i\varphi}$, referred to as the *global phase*, are experimentally indistinguishable. In this sense, states are one dimensional spaces represented by a class of vectors of length one.

The natural basis of quantum informatics is a quantum system with two basis states, which are analogous to 0 and 1 used in classical information theory. Such a system is therefore called *qubit* and its basis states are denoted $|0\rangle$and $|1\rangle$. Taking into account the projective equivalence, the qubit is mathematically the *complex projective line* $\mathbb{P}^1(\mathbb{C})$. But we will more often denote it as $\mathbb{H}_2$ (thus ignoring the phase equivalence of states).

Postulate 2. The time evolution of the isolated quantum system $|u(t)\rangle$ is given by differential equation

$$i\hbar\frac{\partial}{\partial t}|u(t)\rangle = H|u(t)\rangle,$$

where $\hbar \in \mathbb{R}$ is the so-called reduced Planck constant and H is an Hermitian operator, called the *Hamiltonian* of the system.

This equation is called *Schrödinger's equation.* The physical significance of the Planck constant is the ratio between the energy and frequency of a photon. Since it is a real number, it is possible to omit it from the equation (and consider the Hamiltonian divided by this constant). Since Hamiltonian is Hermitian, Schrödinger's equation has a simple form for its eigenvectors (we omit the Planck constant)

$$\frac{\partial}{\partial t}|u(t)\rangle = -ir|u(t)\rangle,$$

where $r \in \mathbb{R}$ is the eigenvalue of the operator H. Assuming that the Hamiltonian does not change over time, it is easy to find a solution for the eigenvector $|u(t)\rangle$

$$|u(t)\rangle = e^{-irt}|u(t_0)\rangle.$$

Using our convention about functions of operators, we get a notation for the general vector $|v\rangle$

$$|v(t)\rangle = e^{-iHt}|v(t_0)\rangle.$$

It is easy to see that the operator e^{-iHt} has eigenvalues of size one (namely e^{-irt}), and is therefore unitary.

Because in quantum computers we want to perform precisely defined discrete operations on the input (on the input qubites), we can reformulate the second postulate in discrete form as follows:

Postulate 2'. The quantum state of an isolated quantum system $|\varphi\rangle$ changes during a time interval Δt to the state $U|\varphi\rangle$, where U is a unitary operator.

Postulate 3. A measurement is given by a Hermitian operator M, called *observable.* Let

$$M = \sum_i m_i P_i$$

be the spectral decomposition of M (i.e, m_i are the eigenvalues of M and P_i projections on the eigenspace corresponding to the eigenvalue m_i).

– The result of the measurement is one of the numbers m_i (which is real because the operator is Hermitian).
– The probability that the result of measuring the state $|\varphi\rangle$ will be $m_i$is equal to $\langle\varphi|P_i|\varphi\rangle$.
– If the result of the state measurement $|\varphi\rangle$ is equal to m_i, the system immediately after the measurement is in the state

$$\frac{P_i|\varphi\rangle}{\sqrt{\langle\varphi|P_i|\varphi\rangle}}$$

(we say the system *collapses* into this state).

This postulate describes the so-called *projective measurement* and does not describe the phenomenon of quantum measurement in general. For our purposes, however, this will be enough, moreover, it is true that each measurement can be converted to projective measurements with certain modifications. In the so-called *non-degenerate* case, the number of different eigenvalues is equal to the dimension of the system (there are no multiple eigenvalues) and all the mentioned subspaces are one-dimensional. Degenerate measurement is therefore characterized by the fact that the number of possible results is smaller than the dimension of the system, i.e. smaller than the measurement of other quantities. Note that we the dimension of the system is the maximum number of possible measurement results.

Note that the measurement is given by a set of projection operators P_i. Which one of them will be used is a random phenomenon determining the measurement result. The probability that the operator P_i will be used is given by the square of the size of the projection result, i.e. the square of the norm of the vector $P_i|\varphi\rangle$. This is equal to $\langle\varphi|P_i^\dagger P_i|\varphi\rangle$, which is equal to $\langle\varphi|P_i|\varphi\rangle$ since the projection is Hermitian and idempotent. Since $|\varphi\rangle = \sum_i P_i|\varphi\rangle$ holds, the sum of all probabilities is equal to one for a unit vector.

The result of the projection is standardized in the above formula by the square root of the probability of the result. Note that the normalization factor $|\varphi\rangle$ depends on the vector and causes the measurement to be a nonlinear mapping.

Each measurement captures some property of the system. The Hamiltonian, which occurs in the Schrödinger equation, for example, corresponds to the so-called total energy of the system (the time evolution of the system is therefore determined by this quantity).

Since the observable is Hermitian, it has an orthonormal basis of eigenvectors $|\mathbf{b}_i\rangle$. The projection on subspace P_i is then equal to

$$P_i = \sum_j |\mathbf{b}_j\rangle\langle\mathbf{b}_j|,$$

where we sum over all base vectors with eigenvalue m_i.

Writing the observable as one operator (i.e. not, for example, as a set of projections) enables, among other things, fast calculation of the mean value of the observable M on a specific state $|\varphi\rangle$ as

$$\mathbf{E}(M) = \sum_i m_i p(m_i) = \sum_i m_i\langle\varphi|\mathbf{b}_i\rangle\langle\mathbf{b}_i|\varphi\rangle = \langle\varphi|(\sum_i m_i|\mathbf{b}_i\rangle\langle\mathbf{b}_i|)|\varphi\rangle = \langle\varphi|M|\varphi\rangle.$$

Postulate 4. Let U and V be quantum systems. Then a system composed of U and V is described by the tensor product $U \otimes V$. If the system U is in the state

$|u\rangle$ and the system V is in the state $|v\rangle$, then the state of the compound system is equal to $|u\rangle \otimes |v\rangle$.